

# **EXHIBIT H**

# BLANKROME

444 West Lake Street | Suite 1650 | Chicago, IL 60606

*Phone:* (312) 776-2518

*Fax:* (312) 276-2601

*Email:* [rachel.schaller@blankrome.com](mailto:rachel.schaller@blankrome.com)

December 6, 2024

**VIA ELECTRONIC MAIL AND  
FEDERAL EXPRESS DELIVERY**

Tekion Corporation  
Attn: Aysswarya Murthi  
Deputy General Counsel  
12647 Alcosta Blvd., Suite 230  
San Ramon, CA 94583  
[aysswarya@tekion.com](mailto:aysswarya@tekion.com)

Fenwick & West LLP  
Attn: Armen Nercessian  
555 California Street, #12  
San Francisco, CA 94104  
[anercessian@fenwick.com](mailto:anercessian@fenwick.com)

**Re: Cease and Desist/Notice of Legal Action**

Dear Ms. Murthi and Mr. Nercessian,

This firm represents CDK Global, LLC (“CDK”). We are writing to demand that Tekion Corporation (“Tekion”) immediately cease and desist from engaging in activities that violate CDK’s rights and various state and federal laws, as previously outlined in CDK’s letters. We further demand that Tekion identify to CDK all customers for which Tekion has accessed and/or downloaded information from CDK’s computer systems, including CDK’s DMS, within seven (7) days of receiving this letter. CDK reserves all rights.

**Unauthorized Access to and Use of CDK's Dealer Management System (DMS)**

CDK has obtained ample evidence that Tekion is accessing, utilizing, and extracting data from CDK’s DMS without authorization. This unauthorized access includes the use of software scripts and establishing secret VPNs, which violates multiple state and federal laws.

In April 2021, CDK and Tekion entered into a Conversion Support Agreement (the “CSA”) to create a reciprocal process by which CDK and Tekion could transfer customer data, standardizing dealership conversions from one DMS provider to the other. While the term of the CSA expired, CDK continued to provide reasonable assistance to Tekion during the conversion process, including by creating custom code for dealers converting their DMS from CDK to Tekion, and on certain occasions, accommodating Tekion’s requests to modify the code to better assist it in the conversion process.

Tekion has chosen to circumvent the CDK-facilitated conversion process, gain unauthorized, administrative access to CDK’s DMS, and run software scripts to extract large

Blank Rome LLP | [blankrome.com](http://blankrome.com)

# BLANKROME

December 6, 2024

Page 2

volumes of data. CDK has detected several new user accounts bearing variations of the name “tekion,” which are run through the same two virtual desktops. We have discovered that Tekion is inducing CDK dealership customers to create and provide Tekion login credentials with administrative access to the DMS, without CDK’s permission and in clear violation of dealers’ agreements with CDK. We understand that prior communications between Tekion and CDK have already put Tekion on notice that this conduct is strictly prohibited. Our investigation has uncovered that Tekion has ignored our prior notice and used covert means to create new accounts after CDK disabled prior ones.

Further, we have reason to believe that, once on CDK’s DMS, Tekion has created reports to extract dealership data – sometimes using scripts to create hundreds or thousands of reports at a time. The use of third-party software scripts to access and utilize CDK’s DMS in this manner is both a violation of dealers’ agreements with CDK and creates significant security risks for CDK and degrades system performance. With administrative access, Tekion would also have the ability to damage CDK’s DMS by deleting customer data or accounts, and otherwise accessing dealership financial and sensitive data and exposing it to corruption and security risk.

Tekion steadfastly has adapted its practices to evade detection of its repeated access to CDK’s DMS from virtual desktops. Most recently, CDK has become aware that Tekion sought to establish a VPN at CDK’s dealer’s location to establish a secret network connection onto which it can create reports and extract data from CDK’s DMS.

## **Violations of State and Federal Laws**

Based on the evidence gathered to date, CDK has reason to believe that Tekion is engaged in the persistent violation of multiple state and federal laws that prohibit Tekion’s illegal hacking and computer fraud, privacy, copyright infringement, misappropriation, unfair and deceptive trade practices, and tortious interference with contract. Violation of these laws exposes Tekion to civil and criminal penalties, including liability for statutory damages, actual damages, attorneys’ fees and injunctive relief.

Specifically, CDK has agreements with various dealership clients that detail the steps the dealership must take before their data may be exported for conversion to a new DMS provider. These agreements impose certain obligations on the dealerships to maintain the confidentiality of CDK’s products and services, and prohibits them from granting third-party access to CDK’s products or systems, using software or other automated means to extract data, and recompiling data in order to reverse engineer any CDK product. Further, under these agreements, the dealerships are required to fulfill the term of the agreement or make certain payments to CDK before CDK is obligated to assist with the conversion of dealership data to a new DMS provider.

Tekion’s actions, including its remote or in-person access to CDK’s products and services, inducement of dealerships to provide Tekion direct access to CDK’s DMS, use of automated scripts to extract data from CDK’s DMS, and surreptitious creation of VPN “tunnels” to the DMS tortiously interferes with CDK’s contractual rights with its dealerships and violates numerous state and federal statutes. CDK has been significantly harmed by these

# BLANKROME

December 6, 2024

Page 3

activities. This harm includes certain dealerships' decision not to perform conditions precedent to data conversion, avoiding significant payment obligations which remain due and owing to CDK. These payments may be recovered from Tekion as damages due to its tortious interference with dealers' contractual obligations to CDK and under state and federal computer fraud, privacy, anti-hacking and deceptive trade practices laws.

## **Demand for Immediate Cessation, Certification and Document Preservation**

CDK demands that Tekion (i) immediately cease and desist all unauthorized access to CDK's DMS, (ii) within seven (7) days, (a) identify each account it has created on CDK's DMS and each dealership whose CDK DMS it has accessed, and (b) certify in writing that it has disabled all accounts to CDK's DMS that it has created or otherwise has access to, and (iii) refrain from creating any new accounts or using dealership credentials to gain direct access to a CDK DMS or other CDK computer system unless it receives prior written authorization from CDK's general counsel.

Finally, this letter puts Tekion on notice of threatened or impending litigation concerning the allegations contained herein. Tekion must preserve all relevant evidence, suspend any routine data deletion policies, retention schedules or automated systems that might overwrite relevant information, and otherwise ensure that no data within these categories is altered, deleted, or destroyed:

1. **Access to CDK DMS:** Any actions taken to access, download, use, receive, modify, transmit, or otherwise process information from the CDK DMS.
2. **Communications Regarding CDK DMS:** All communications, including but not limited to emails, instant messages, text messages, phone logs, or other records, that discuss or relate to the CDK DMS.
3. **Dealership Data:** Any actions involving the use, receipt, modification, processing, or transmission of data related to CDK's customers, including all dealership management data derived from or connected to CDK systems.
4. **Communications with Client Dealerships:** Any and all communications (including emails, text messages, social media messages, call logs, and meeting notes) with dealerships regarding the transfer of services, data, or accounts related to the CDK DMS or dealership management data.

This preservation requirement includes, but is not limited to, the following categories of data:

1. **Electronic Devices:** Any computer, laptop, tablet, mobile device, server, or other electronic device used for any of the above purposes.
2. **Cloud and Virtual Systems:** Any cloud accounts, virtual machines, or cloud-based storage systems where relevant data may be stored.

# BLANKROME

December 6, 2024

Page 4

3. **Electronic Communications:** Emails, text messages, instant messages, and other digital communications.
4. **Files and Documents:** Any digital or physical files, documents, spreadsheets, or logs.
5. **Scripts and Automation:** Any scripts, automation tools, or software used to access, process, or manipulate data from CDK systems.
6. **Backups and Snapshots:** Any backups, images, or snapshots of devices or accounts that may contain relevant data.

CDK reserves all rights concerning Tekion's ongoing and prior unlawful conduct.

Very truly yours,



Rachel L. Schaller

cc: Cameron Williams, EVP, General Counsel and Secretary  
Daniel R. Saeedi, Attorney